AMENDMENTS TO THE CLAIMS

1.   (Cancelled)

2.   (Currently amended) A method of generating an identity authentication code associated with an authentication device, comprising:

        providing event state data representing an occurrence of a reportable event concerning that specifies a condition of the authentication device; and,

        generating an identity authentication code that depends on (i) the event state data, and (ii) a secret associated with the device.

3.   (Previously presented) The method of claim 2, wherein the identity authentication code further depends on a dynamic value.

4.   (Previously presented) The method of claim 3, wherein the dynamic value includes one or more of a time value, a challenge, and a counter.

5.   (Previously presented) The method of claim 2, wherein the condition of the authentication device includes information about whether the device has been subjected to tampering.

6.   (Previously presented) The method of claim 2, further including changing the event state data when the condition of the authentication device changes.

7.   (Previously presented) The method of claim 2, wherein the condition of the device is covertly encoded in the identity authentication code.

8.   (Previously presented) The method of claim 2, wherein the event state data is derived from an associated event secret.

9.   (Previously presented) The method of claim 8, further including periodically changing the event secret.

2

10.   (Previously presented) The method of claim 8, further including changing the event secret each time the dynamic value changes.

11.   (Previously presented) The method of claim 5, further including changing the event secret when the condition of the authentication device changes.

12.   (Previously presented) The method of claim 2, wherein the event state data includes one or more event state bits, a subset of bits being employed in generating identity authentication codes for different time intervals.

13.   (Previously presented) The method of claim 2, further including generating the event state data using a funkspiel scheme.

14.   (Previously presented) The method of claim 2, wherein the condition of the authentication device includes information about whether a battery supplying power to the authentication device has fallen below an expected power level.

15.   (Previously presented) The method of claim 2, wherein the condition of the authentication device includes information the likelihood that the authentication device has or will develop an operational problem.

16.   (Previously presented) The method of claim 15, wherein the operational problem is a device reset.

17.   (Previously presented) The method of claim 2, wherein the identity authentication code further depends on of one or more of a PIN, a password, data derived from a biometric observation, user data, verifier data, and a generation value.

18.   (Previously presented) The method of claim 2, further including, before generating the authentication code, receiving user input data, wherein the user input data is at least one of a PIN, a password, and biometric data.

19.   (Previously presented) The method of claim 18, further including, before generating the authentication code, verifying whether the user input data is correct, and providing the identity authentication code only if the user input data is verified to be correct.

20.   (Previously presented) The method of claim 2, further including transmitting the identity authentication code to a verifier.

21.   (Previously presented) The method of claim 20, further including receiving, by the verifier, authentication information comprising the identity authentication code; and,

    determining, by the verifier, the correctness of the identity authentication code and the event state data.

22.   (Previously presented) The method of claim 20, wherein the verifier includes a representation of the secret associated with the device.

23.   (Previously presented) The method of claim 21, wherein the authentication information further includes a user identifier.

24.   (Previously presented) The method of claim 20, wherein the authentication information further includes at least one of a PIN, a password, and biometric data.

25.   (Previously presented) The method of claim 2, further including the step of displaying the identity authentication code on the device.

26.   (Previously presented) A method of generating an identity authentication code associated with an authentication device, comprising:

4

providing event state data that is a security indicator for an authentication system of which the authentication device is a component; and,

generating an identity authentication code that depends on (i) the event state data, and (ii) a secret associated with the device.

27.   (Previously presented) The method of claim 26, wherein the identity authentication code further depends on a dynamic value.

28.   (Previously presented) The method of claim 27, wherein the dynamic value includes one or more of a time value, a challenge, and a counter.

29.   (Previously presented) The method of claim 26, wherein the security indicator includes information regarding strength of a biometric match.

30.   (Previously presented) The method of claim 26, wherein the security indicator includes information regarding accuracy of a PIN entry.

31.   (Previously presented) The method of claim 26, wherein the security indicator includes information regarding a device type associated with the authentication device.

32.   (Previously presented) The method of claim 26, wherein the security indicator includes information regarding a device signature or pattern associated with the authentication device.

33.   (Previously presented) The method of claim 26, wherein the security indicator includes information regarding a length of time the authentication device has been inserted into a device reader.

34.   (Previously presented) The method of claim 26, wherein the security indicator includes information regarding a protection level of the secret associated with the device.

35.   (Previously presented) The method of claim 26, wherein the identity authentication code further depends on one or more of a PIN, a password, data derived from a biometric observation, user data, verifier data, and a generation value.

36.   (Previously presented) The method of claim 26, further including, before generating the authentication code, receiving user input data, wherein the user input data is at least one of a PIN, a password, and biometric data.

37.   (Previously presented) The method of claim 36, further including, before generating the authentication code, verifying whether the user input data is correct, and providing the identity authentication code only if the user input data is verified to be correct.

38.   (Previously presented) The method of claim 26, further including transmitting the identity authentication code to a verifier.

39.   (Previously presented) The method of claim 38, further including receiving, by the verifier, authentication information comprising the identity authentication code; and,

determining, by the verifier, the correctness of the identity authentication code and the event state data.

40.   (Previously presented) The method of claim 38, wherein the verifier includes a representation of the secret associated with the device.

41.   (Previously presented) The method of claim 39, wherein the authentication information further includes a user identifier.

42.   (Previously presented) The method of claim 39, wherein the authentication information further includes at least one of a PIN, a password, and biometric data.

43.   (Previously presented) A method of generating an identity authentication code associated with an authentication device, comprising:

providing event state data that specifies information about a user of the authentication device; and,

generating an identity authentication code that depends on (i) the event state data, and (ii) a secret associated with the device.

44.   (Previously presented) The method of claim 43, wherein the identity authentication code further depends on a dynamic value.

45.   (Previously presented) The method of claim 44, wherein the dynamic value includes one or more of a time value, a challenge, and a counter.

46.   (Previously presented) The method of claim 43, wherein the information about the user includes whether the user is stationary or in motion.

47.   (Previously presented) The method of claim 43, wherein the information about the user includes where the user is located.

48.   (Previously presented) The method of claim 47, wherein the information regarding where the user is located includes geographical position.

49.   (Previously presented) The method of claim 43, wherein the identity authentication code further depends on one or more of a PIN, a password, data derived from a biometric observation, user data, verifier data, and a generation value.

50.   (Previously presented) The method of claim 43, further including, before generating the authentication code, receiving user input data, wherein the user input data is at least one of a PIN, a password, and biometric data.

51.   (Previously presented) The method of claim 50, further comprising, before generating the authentication code, verifying whether the user input data is correct, and providing the identity authentication code only if the user input data is verified to be correct.

52.   (Previously presented) The method of claim 43, further including transmitting the identity authentication code to a verifier.

53.   (Previously presented) The method of claim 52, further including receiving, by the verifier, authentication information comprising the identity authentication code; and,

        determining, by the verifier, the correctness of the identity authentication code and the event state data.

54.   (Previously presented) The method of claim 52, wherein the verifier includes a representation of the secret associated with the device.

55.   (Previously presented) The method of claim 53, wherein the authentication information further includes a user identifier.

56.   (Previously presented) The method of claim 53, wherein the authentication information further includes at least one of a PIN, a password, and biometric data.

57.   (Previously presented) A method of generating an identity authentication code associated with an authentication device, comprising:

        providing event state data that specifies information about environmental conditions associated with the authentication device; and,

        generating an identity authentication code that depends on (i) the event state data, and (ii) a secret associated with the device.

8

58.   (Previously presented) The method of claim 57, wherein the identity code further depends on a dynamic value.

59.   (Previously presented) The method of claim 58, wherein the dynamic value includes one or more of a time value, a challenge, and a counter.

60.   (Previously presented) The method of claim 57, wherein the information includes temperature characteristics associated with the authentication device.

61.   (Previously presented) The method of claim 60, wherein the temperature characteristics include an ambient temperature to which the authentication device is exposed.

62.   (Previously presented) The method of claim 60, wherein the temperature characteristics include a temperature of a component of the authentication device.

63.   (Previously presented) The method of claim 57, wherein the information includes radiation levels to which the authentication device as been exposed.

64.   (Previously presented) The method of claim 57, wherein the information indicates whether static discharge to the device has occurred.

65.   (Previously presented) The method of claim 57, wherein the identity authentication code further depends on one or more of a PIN, a password, data derived from a biometric observation, user data, verifier data, and a generation value.

66.   (Previously presented) The method of claim 57, further including, before generating the authentication code, receiving user input data, wherein the user input data is at least one of a PIN, a password, and biometric data.

67.   (Previously presented) The method of claim 66, further comprising, before generating the authentication code, verifying whether the user input data is correct, and providing the identity authentication code only if the user input data is verified to be correct.

68.   (Previously presented) The method of claim 57, further including transmitting the identity authentication code to a verifier.

69.   (Previously presented) The method of claim 68, further including receiving, by the verifier, authentication information comprising the identity authentication code; and,

      determining, by the verifier, the correctness of the identity authentication code and the event state data.

70.   (Previously presented) The method of claim 68, wherein the verifier includes a representation of the secret associated with the device.

71.   (Previously presented) The method of claim 69, wherein the authentication information further includes a user identifier.

72.   (Previously presented) The method of claim 69, wherein the authentication information further includes at least one of a PIN, a password, and biometric data.

73.   (Currently amended) A method for verifying the correctness of an identity authentication code, comprising:

      receiving authentication information including the identity authentication code generated by an authentication device that depends on (i) a secret associated with the device, and (ii) event state data representing an occurrence of a reportable event concerning that specifies a condition of the authentication device;

      verifying the correctness of the identity authentication code, and determining the condition of the authentication device in response to the received identity authentication code.

74.   (Previously presented) The method of claim 73, further including taking an action in response to the event state.

75.   (Previously presented) The method of claim 73, further including determining whether an event occurred in response to the determined event state.

76.   (Previously presented) The method of claim 73, wherein the event is tampering with the device.

77.   (Previously presented) The method of claim 73 wherein the condition of the device is covertly encoded in the authentication code.

78.   (Previously presented) The method of claim 73, wherein the authentication information further includes a user identifier.

79.   (Previously presented) The method of claim 78, wherein the authentication information further includes at least one of a PIN, a password, and biometric data.

80.   (Previously presented) The method of claim 73, wherein the verifying the correctness of the identity authentication code further includes generating an expected identity authentication code that depends an expected event state data.

81.   (Previously presented) The method of claim 73, wherein the verifying the correctness of the identity authentication code further includes recovering the event state data from the identity authentication code.

82.   (Previously presented) The method of claim 80, wherein the event state data includes one or more event state bits, a subset of bits being employed in generating identity authentication codes for different time interval.

83.   (Previously presented) A method for verifying the correcteness of an identity authentication code, comprising:

receiving authentication information including the identity authentication code generated by an authentication device that depends on (i) a secret associated with the device, and (ii) event state data that is a security indicator for an authentication system of which the authentication device is a component;

verifying the correctness of the identity authentication code, and determining the event state data in response to the received identity authentication code.

84.   (Previously presented) A method for verifying the correctness of an identity authentication code, comprising:

receiving authentication information including an identity authentication code generated by an authentication device that depends on (i) a secret associated with the device, and (ii) event state data that specifies information about a user of the authentication device;

verifying the correctness of the identity authentication code, and determining the event state data in response to the received identity authentication code.

85.   (Previously presented) A method for verifying the correctness of an identity authentication code, comprising:

receiving authentication information including an identity authentication code generated by an authentication device that depends on (i) a secret associated with the device, and (ii) event state data that specifies information about environmental conditions associated with the authentication device;

verifying the correctness of an identity authentication code, and determining the event state data in response to the received identity authentication code.

12